

Appl. No. 09/275,722

Attorney Docket: 042390.P6526

LISTING OF THE CLAIMS:

This listing of claims replaces all prior versions, and listings, of claims in the application:

- 1 (Previously Presented) 1. A method comprising:
2 providing a key matrix having N rows and M columns of matrix keys, where $N \geq 2$ and
3 $M \geq 2$;
4 for each column of the key matrix, performing arithmetic operations utilizing matrix keys
5 of at least two selected rows of the key matrix to produce a secret device key which is part of a
6 first set of secret device keys;
7 producing a shared secret key based on arithmetic operations on selected secret device
8 keys of the first set of secret device keys.
- 1 (Original) 2. The method of claim 1, wherein the arithmetic operations include modular
2 addition.
- 1 (Original) 3. The method of claim 1, wherein prior to performing the arithmetic operations, the
2 method comprises:
3 generating a key selection vector identifying the at least two selected rows of the key
4 matrix from which to produce the first set of secret device keys.
- 1 (Original) 4. The method of claim 3, wherein the key selection vector is uniquely assigned to a
2 first digital platform.

Appl. No. 09/275,722

Attorney Docket: 042390.P6526

1 (Original) 5. The method of claim 4, wherein prior to producing the shared secret key, the
2 method comprises:
3 receiving a key selection vector from a second digital platform in communication with
4 the first digital platform; and
5 analyzing contents of the key selection vector from the second digital platform to
6 determine the selected secret device keys of the first set of secret device keys.

1 (Original) 6. The method of claim 1, wherein prior to performing arithmetic operations on keys
2 of at least two selected rows, the method further comprises:
3 dedicating the rows of the key matrix to a first classification; and
4 dedicating the columns of the key matrix to a second classification.

1 (Original) 7. The method of claim 6, wherein the first classification includes digital platforms
2 designed to provide information to other digital platforms.

1 (Original) 8. The method of claim 7, wherein the second classification includes digital
2 platforms designed to receive information from other digital platforms.

1 (Original) 9. The method of claim 1, wherein the producing of the shared secret key comprises:
2 analyzing contents of an incoming key selection vector; and
3 performing arithmetic operations of the selected secret device keys located in columns of
4 the key matrix identified by the contents of the incoming key selection vector.

Appl. No. 09/275,722

Attorney Docket: 042390.P6526

1 (Original) 10. The method of claim 9, wherein the producing of the shared secret key further
2 comprises:
3 performing a hash operation on results of the arithmetic operations of the selected secret
4 device keys located in the column of the key matrix identified by the contents of the
5 incoming key selection vector.

1 (Previously Presented) 11. A method comprising:
2 providing a key matrix having N rows and M columns of matrix keys, where $N \geq 2$ and
3 $M \geq 2$;
4 for each row of the key matrix, performing arithmetic operations utilizing matrix keys of
5 at least two selected columns of the key matrix to produce a secret device key which is part of a
6 first set of secret device keys;
7 producing a shared secret key based on arithmetic operations on selected secret device
8 keys of the first set of secret device keys.

1 (Original) 12. The method of claim 11, wherein the arithmetic operations include modular
2 addition.

1 (Previously Presented) 13. The method of claim 11, wherein prior to performing the
2 arithmetic operations, the method comprises:
3 generating a key selection vector identifying the at least two selected columns of the key
4 matrix from which to produce the first set of secret device keys.

Appl. No. 09/275,722

Attorney Docket: 042390.P6526

1 (Original) 14. The method of claim 13, wherein the key selection vector is uniquely assigned to
2 a first digital platform.

1 (Original) 15. The method of claim 14, wherein prior to producing the shared secret key, the
2 method comprises:
3 receiving a key selection vector from a second digital platform in communication with
4 the first digital platform; and
5 analyzing contents of the key selection vector from the second digital platform to
6 determine the selected secret device keys of the first set of secret device keys.

1 (Previously Presented) 16. The method of claim 11, wherein prior to performing arithmetic
2 operations on keys of at least two selected columns, the method further comprises:
3 dedicating the rows of the key matrix to a first classification; and
4 dedicating the columns of the key matrix to a second classification.

1 (Original) 17. The method of claim 11, wherein the producing of the shared secret key
2 comprises:
3 analyzing contents of an incoming key selection vector; and
4 performing arithmetic operations of the selected secret device keys located in rows of the
5 key matrix identified by the contents of the incoming key selection vector.

1 (Original) 18. The method of claim 17, wherein the producing of the shared secret key further
2 comprises:

Appl. No. 09/275,722

Attorney Docket: 042390. P6526

3 performing a hash operation on results of the arithmetic operations of the selected secret
4 device keys located in the rows of the key matrix identified by the contents of the incoming key
5 selection vector.

1 (Original) 19. A machine readable medium having embodied thereon a computer program for
2 processing by a first digital platform including memory containing the computer program
3 comprising:

4 an authentication function to recover an incoming key selection vector and to compute a
5 shared secret key based on a set of secret device keys stored in the first digital platform and the
6 contents of the incoming key selection vector;

7 a transfer function to output at least a key selection vector assigned to the first digital
8 platform;

9 a hash function to perform a hash operation on at least the shared secret key to produce a
10 resultant hash value; and

11 a comparison function to compare the resultant hash value with an incoming check hash
12 value received subsequent to the transmission of the key selection vector.

1 (Original) 20. A network comprising:

2 a first digital platform; and

3 a certification authority in communication with the first digital platform, the certification
4 authority having access to a key matrix featuring matrix keys arranged in accordance with at
5 least a first dimension and a second dimension, generating a first key selection vector and
6 providing a first set of secret device keys produced from selected matrix keys of the key matrix.

Appl. No. 09/275,722

Attorney Docket: 042390. P6526

1 (Original) 21. The network of claim 20 further comprising:
2 a second digital platform in communication with the certification authority and the first digital
3 platform, the second digital platform being uniquely assigned a second key selection vector
4 indicating at least two grids of the key matrix and a second set of secret device keys produced
5 from matrix keys situated in at least two grids of the key matrix.

1 (Original) 22. The network of claim 21, wherein the first and second digital platforms to
2 exchange the first and second key selection vectors in order for each digital platform to produce
3 a shared secret key to ensure that communications between the first and second digital platforms
4 are secure.

1 (Original) 23. A certification authority comprising:
2 a memory to store a key matrix having N rows and M columns of matrix keys, where
3 $N \geq 2$ and $M \geq 2$;
4 a logic to generate a key selection vector for each digital platform registered with the
5 certification authority.

1 (Original) 24. The certification authority of claim 23, wherein the logic includes a processing
2 unit.

1 (Original) 25. The certification authority of claim 24, wherein the processing unit produces a
2 first set of secret device keys by performing arithmetic operations on matrix keys along selected

Appl. No. 09/275,722

Attorney Docket: 042390. P6526

3 columns of the key matrix identified by the key selection vector to provide a first set of secret
4 device keys to a digital platform.

1 (Original) 26. The certification authority of claim 25, wherein the matrix keys along the
2 processing unit performs arithmetic operations on matrix keys along selected rows of the key
3 matrix identified by the key selection vector to provide a first set of secret device keys to a
4 digital platform.

1 (Original) 27. The certification authority of claim 23, wherein the matrix keys are only known
2 by the certification authority.